

Best Available Copy

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-304808

(43)Date of publication of application : 18.10.2002

(51)Int.Cl. G11B 20/10
 G06F 1/00
 G06F 12/14
 G11B 7/004
 G11B 7/007
 G11B 20/12

(21)Application number : 2002-018467

(71)Applicant : EASTMAN KODAK CO

(22)Date of filing : 28.01.2002

(72)Inventor : BARNARD JAMES A
 INCHALK MICHAEL A
 HA BRUCE L

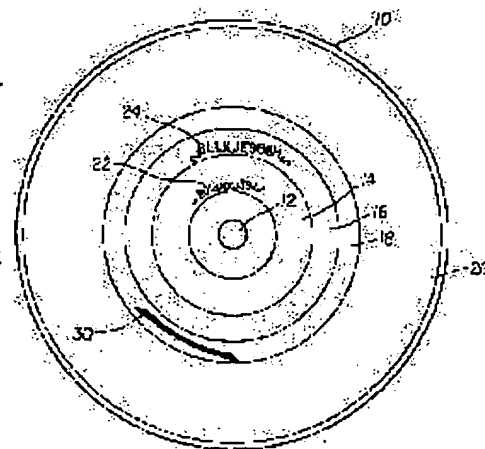
(30)Priority

Priority number : 2001 772149 Priority date : 29.01.2001 Priority country : US

(54) COPY PROTECTION USING MULTIPLE SECURITY LEVELS ON A PROGRAMMABLE CD-ROM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for making copy protection that cannot be subverted by a bit-for-bit copying scheme on standard CD-writers.
 SOLUTION: This invention provides a copy-protected optical disk, including a pre-formed identification number (ID) in the ATIP(Absolute Time In Pre-groove) signal and the subcode which is impressed upon the optical disk and a number of other optical disks during optical disk manufacture, a unique identification number for the optical disk which was written on the optical disk after it is manufactured, and an encrypted program written onto the optical disk wherein the encryption of such program is based upon the performed ID and the unique ID and includes two or more selectable security levels.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-304808

(P2002-304808A)

(43) 公開日 平成14年10月18日 (2002. 10. 18)

(51) Int. Cl. ⁷	識別記号	F I	テームト* (参考)
G 1 1 B 20/10	3 0 1	G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 1/00	3 2 0	G 0 6 F 12/14	3 0 1 Z 5 B 0 7 6
12/14		G 1 1 B 7/004	3 2 0 F 5 D 0 4 4
G 1 1 B 7/004		7/007	Z 5 D 0 9 0

審査請求 未請求 請求項の数 6 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2002-18467 (P2002-18467)

(22) 出願日 平成14年1月28日 (2002. 1. 28)

(31) 優先権主張番号 7 7 2 1 4 9

(32) 優先日 平成13年1月29日 (2001. 1. 29)

(33) 優先権主張国 米国 (U S)

(71) 出願人 590000846

イーストマン コダック カンパニー

アメリカ合衆国, ニューヨーク14650, ロ

チェスター, ステイト ストリート343

(72) 発明者 ジェイムズ エイ パーナード

アメリカ合衆国 ニューヨーク 14546

スコッツヴィル チリ・アヴェニュー 51

(72) 発明者 マイケル エイ インチャリック

アメリカ合衆国 ニューヨーク 14534

ピッツフォード カッパー・ウッズ 30

(74) 代理人 100070150

弁理士 伊東 忠彦

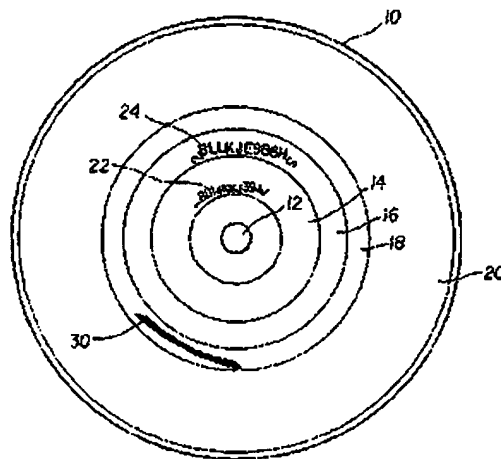
最終頁に続く

(54) 【発明の名称】 プログラム可能なCD-ROMにおける多重セキュリティ・レベルを利用するコピー・プロテクト

(57) 【要約】

【課題】 標準的なCDライターでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供すること。

【解決手段】 本発明によれば、コピー・プロテクトされた光学ディスクが提供される。光学ディスクは、A T I P信号およびサブコード内の予め形成された識別番号 (I D) であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号 (I D) と、製造された後に光学ディスクに書き込まれた光学ディスクに関する固有の識別番号と、光学ディスクに書き込まれた暗号化されたプログラムより成る。そのプログラムの暗号化は、予め形成されたI Dおよび固有のI Dに基づいて行われ、および2つまたはそれ以上の選択可能なセキュリティ・レベルを有する。



(2)

特開2002-304808

1

2

【特許請求の範囲】

【請求項1】 コピー・プロテクトされた光学ディスクであって：

a) A T I P信号およびサブコード内の予め形成された識別番号（ID）であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号（ID）；

b) 製造された後に前記光学ディスクに書き込まれた前記光学ディスクに関する固有の識別番号；および

c) 前記光学ディスクに書き込まれた暗号化されたプログラム；より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび前記固有のIDに基づいて行われ、および2つまたはそれ以上の選択可能なセキュリティ・レベルを有することを特徴とするコピー・プロテクトされた光学ディスク。

【請求項2】 主チャネル・データ・ストリームに記された前記予め形成された形成されたIDを有することを特徴とする請求項1記載のコピー・プロテクトされた光学ディスク。

【請求項3】 光学ディスクに記録された情報をコピー・プロテクトする方法であって：

a) A T I P信号およびサブコードに記録された予め形成された識別番号（ID）を包含するマスタ・ディスクを形成し、前記マスタ・ディスクと同一のIDを有する複数の光学ディスクを形成するステップ；

b) 光学ディスクに関する固有のIDを光学ディスクに書き込むステップ；および

c) 前記光学ディスクに暗号化されたプログラムを書き込むステップ；より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび前記固有の識別番号に基づいて行われることを特徴とする方法。

【請求項4】 前記予め形成されたIDが前記データ・ストリームに記録されていることを特徴とする請求項3記載の方法。

【請求項5】 前記予め形成されたIDが、前記ディスクに関する最大の開始および導出の開始情報を含み、前記A T I P信号の特殊情報に記録されることを特徴とする請求項3記載の方法。

【請求項6】 更に、前記ディスクから前記予め形成されたIDおよび前記固有のIDを読み出すステップ、および前記予め形成されたIDおよび前記固有のIDを利用して、暗号化されたプログラムの暗号化を解除するステップより成ることを特徴とする請求項3記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンパクト・ディスクその他の光学的に記録されたディスクに記録された情報に対するコピー・プロテクトに関する。

【0002】

【従来の技術】オーディオ、映像、ソフトウェアまたは

データを含む光学ディスクの消費者購買層は数十億ドル市場を生み出した。近年における低価格の光学的記録媒体およびドライバの出現は、制限なしにその内容をコピーすることを普及させた。これに対処するために、様々なコピー・プロテクト手法が開発された。しかしながらこれらの手法の内のあるものは、デジタル・データ・ストリームの特徴を利用し、これは精巧な低価格のレコーダにより、ビットに関するコピー（bit-for-bit copy）を利用してコピーされ得る。他には、書き込みおよび読み込みの両者を困難にするように光学ディスクの特徴を変化させるものがある。さらには、ネットワーク接続または2次的な「キー」（key）ディスク手法を使用し、独立した（スタンドアロンの）プロテクトを許容しないものもある。

【0003】Horstmann(U.S. 5,044,469)は、プロテクト・モジュールを利用したソフトウェア保護機構を開示し、これはライセンス・ファイルを読み出し、購入したそのライセンスに基づく規則を実行する。これは論理レベルにおけるソフトウェアを保護し、特に、権利が認められていないソフトウェアの部分に対する保護である。このシステムがコンパクト・ディスクに包含されるならば、標準的なCDライタを利用したそのディスクの再生成は、終ての既存のアクセスに関するコピーを正当なものにするであろう。

【0004】Asai et al(U.S.Re. 35,839)は、データを格納するコンパクト・ディスクにおける識別領域を利用する方法を開示し、これはディスクの他の場所に格納されたデータと比較され、真正であることを確認する。これは論理レベルにおけるデータを保護するが、そのディスクに関する単純なビットに関するコピーによって、そのプロテクトは破られてしまう。

【0005】DeMont(U.S. 5,982,889)は、情報製品（information product）に対するユーザ・アクセスが真正であることを確認する方法を教示する。このシステムの欠点は、その真正確認が中央局を介して行われることである。ネットワークに接続することを希望しない（または不可能な）ユーザは、この製品を利用することができない。

【0006】Hasebe, et al(U.S. 5,555,304)は、ユーザ各自または使用されるコンピュータに関連するシステムを開示する。これは、単独のコンピュータにおけるプログラムの利用を真正のユーザに限定し、ユーザの移動性またはそれらの設備のアップ・グレードを非常に制限する。さらに、この特許は、ディスクの再書き込み不可能な領域に格納されたデータの利用にも関連し、再書き込み不可能なリーフ（leaves）が形成されるその手法は、（「再書き込み不可能な」部分も含めて）データを新たなディスクにコピーする機能を開放する。

【0007】Fite et alによる一連の特許(U.S. 5,400,319, 5,513,169, 5,541,904, 5,805,549, および5,930,

(3)

特開2002-304808

3

215)は、規定可能なコードを生成するようにディスクの小領域から反射層を選択的に除去することによって、光学ディスクに機械的に読み取り可能なシリアル番号コードを形成する方法を開示する。このようなシステムに対する欠点は、この特殊なコードを書き込むために特殊な装置が必要とされることである。

【0008】Kanamaru(U.S. 5,940,505)は、どのようにしてCD-ROMがコピー・プロテクトされるかを教示する。しかしながら、Kanamaruの発明の総ての装置は、ディスク上の情報を解読するために、組み込み回路形式でまたは付加的なコンピュータ・ボード形式で、補助的なハードウェアを要する。

【0009】G Connor et al.による米国特許第5,745,568号は、特定のコンピュータ・システムによって回復されるCD-ROMデータを保全する方法およびシステムを開示する。光学ディスクの領域は、暗号キーとしてのハードウェア識別子を用いて暗号化される。ハードウェア識別子は、選択されたコンピュータ・ハードウェアに関連する。CD-ROMに含まれるソフトウェア・プログラム・ファイルは、暗号キーとしてのハードウェア識別子を利用して暗号化される。CD-ROM上の選択されたソフトウェア・プログラムは、暗号キーとしてのハードウェア識別子を利用するソフトウェア・プログラム・ファイルを解読することによって、その選択されたコンピュータ上でインストールされる。

【0010】Akiyama et al.による米国特許第5,805,699号は、マスタ記憶媒体に記録された著作物ソフトウェアを、合法的な手法で、ユーザのターゲット記憶媒体にコピーさせることを可能にするソフトウェア・コピー・システムを提案する。マスタ記憶媒体（すなわち、CD-ROM）は、ソフトウェア識別子を有し、ターゲット記憶媒体は記憶媒体識別子を有する。これら2つの識別子が中央局に伝送され、中央局はソフトウェア製品をコピーするための権利に関するライセンス（契約）を管理している。中央局において、2つの識別子から第1の署名が生成され、コンピュータ・ユーザに返送される。ユーザのコンピュータにおいて、その2つの識別子から第2の署名が生成される。2つの署名が互いに一致する場合に限って、マスタ記憶媒体からターゲット記憶媒体へソフトウェア・プログラムがコピーされ得る。

【0011】Chandra et al.による米国特許第4,644,493号は、単独のコンピュータで使用する磁気媒体で使用するソフトウェアの配布を制限する方法および装置を開示する。磁気媒体に含まれる当初のソフトウェアは、機械的にコピー不可能である。これは、コンピュータの一部をなす不正操作のきかないコプロセッサに格納されたプログラムを実行することによってそれが修正されるまでその状態が続く。

【0012】Indeck et al.による米国特許第5,740,244号は、磁気媒体上のソフトウェア製品が最初にコンピ

4

ュータに命令することによる改善を開示し、その磁気媒体を挿入すると、その製品の特定の部分の指紋を読み取り、その指紋とその同じ指紋に関して予め記録されていたものとを比較する。指紋が一致していれば、ソフトウェア製品は、コンピュータが更に読み込むことを許容し、そこに格納されているアプリケーション・ソフトウェアを実行可能にする。

【0013】これらの手法に関連して多くの問題が存在する。1つには、これらの多くが「ハック」(hacks)と呼ばれるものに対して無防備なことである。この意味することは、あるユーザが解読する又はそのアプリケーションを利用する方法を判別すると、その種の者にとって、そのアプリケーションへのアクセスを取得する方法を定めることは非常に容易であるということである。特定のハードウェアの組み合わせに依存した特定のアプリケーションを利用することによって、この問題を解決するものもある。その手法は携帯性に関する問題を生み出す。合法的なユーザであっても場所が異なればコンピュータ上のアプリケーションを利用できないのである。ユーザが、例えばアップ・グレードによりハードウェアの構成(configuration)を変更すると、そのアプリケーションは起動することができない。

【0014】

【発明が解決しようとする課題】従って、本発明は、標準的なCDライターでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供することを目的とする。ただし、これは標準的なCDマスタおよびライト設備で実行可能なものである。

【0015】

【課題を解決するための手段】この課題を解決するコピー・プロテクトされた光学ディスクは：

- a) ATIP信号およびサブコード内の予め形成された識別番号(ID)であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号(ID)；
- b) 製造された後に前記光学ディスクに書き込まれた前記光学ディスクに関する固有の識別番号；および
- c) 前記光学ディスクに書き込まれた暗号化されたプログラム；

より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび前記固有のIDに基づいて行われ、および2つまたはそれ以上の選択可能なセキュリティ・レベルを有する光学ディスクである。

【0016】本発明は、一般のハッカによる発見を防止しつつ携帯性をも提供し、認証されているユーザが単独のコンピュータ・システムを利用することに関して制限されないようにする。多くの従来技術とは異なり、ソフトウェアが利用される又はインストールされるときに、接触する権限を付与する中央管理的な権利は必要としない。

(4)

特開2002-304808

5

6

【0017】物理的形態のキー（予め形成されたID）および論理的形態のキー（固有のID）の両者を利用することによって、多くの複製手法を排除する。単純なビットに関する複製(bit-for-bit duplication)が回避される。なぜなら、予め形成されたIDをコピーしないからであり、これはディスク・トラックの物理的構造に符号化されている。複数ユーザまたは複数の顧客の間でのソフトウェアの「共有」が回避される。なぜなら、そのように共有されるソフトウェアは、（よく起こるであろう事態として）両ユーザが予め形成されたIDを利用してディスクを使用しようとする場合であっても、適切な固有のIDなしには走らないからである。その記録手法は、ロック(lock)された実行可能なファイルを形成する。予め形成された多書き込みIDを利用することにより、多段階のセキュリティ（保全）が可能になる。

【0018】

【発明の実施の形態】図1を参照するに、本発明によるコピー・プロテクトされた光学ディスク10が示されている。これはプログラム可能なCD-ROMディスクであり、予め記録されたマスタ領域(mastered pre-recorded area)（ROM領域）および記録可能な領域（RAM領域）の両者を含む。ディスク10を回転指させるための中心軸に関するホール12がある。この特定のプログラム可能なCD-ROMディスクは、マスタ化された第1セッション(session)14を有し；すなわち、マスタ・ディスクが、第1セッション14において供給されるソフトウェアまたはデータを包含して形成され、その後、直接的に又は中間的な「父」および「母」ディスクを介して、ディスク10の多くのコピーに印を付すために使用される。

【0019】プログラム可能なCD-ROMを含む書き込み可能なコンパクト・ディスクは、部分的に溝変調(groove modulation)を使用する。ディスク10は、基板の内側端部から外側端部に伸びる連続的ならせん状トラックを有する。らせん状トラックは通常は溝であり、ディスク10にデータ・チャンネルを提供し、データの読み込みまたは書き込みの最中にディスク10のトラッキング(tracking)をも提供する。溝はその溝に垂直な方向の振動を有し、それゆえに揺動した溝(wobbled groove)または揺動的な溝(wobble groove)としても言及される。データをアドレスおよびプログラムする配置に加えて、プログラム可能なCD-ROM光学記録ディスクのトラック又は溝、溝の変調度は、オレンジ・ブック・パート2仕様1(Orange Book Part II specification)に従って提供されるのが普通である。「オレンジ・ブック・パート2」は、フィリップス・インターナショナルBVにより公表された仕様であり、記録可能なコンパクト・ディスク媒体のキー(key)特性および記録特性を規定する。

【0020】溝の振動周波数は、ブレ・グループにおける絶対時間(ATIP: Absolute Time In Pre-groove)とし

て知られる信号を利用して変調される。ATIPは、光学ディスク10の記録面全体に関するトラックの場所に関する情報を含む。オレンジ・ブック仕様によれば、ATIP信号は22.05kHzのFM信号であり、3150ビット/秒のレートでデータを搬送する。このデータは、毎秒7542ビット・フレームとして特定される。データ領域において、各フレームは、4つの同期ビットと、分カウントを表現する8ビットと、秒カウントを表現する8ビットと、フレーム・カウントを表現する8ビットより成る。分、秒およびフレーム・カウントは、2つの4ビット2進10進数(BCD)より成る。ディスク10のデータ領域において、これらの値の任意のものについての最大値は75であり、各々の最上位ビット(MSB)は常にゼロである。そして、分カウント、秒カウントおよびフレーム・カウントの最上位ビットの3つは、全体として、000の2進値を有する。各フレームの最後の14ビットは、巡回冗長検査(CRC: cyclic redundancy check)誤り保護として提供される。

【0021】直径46mmないし50mmの間のディスク10の領域として定義されるディスク導入領域(lead-in area)において、MSBの値は000から変化する。100という値は、そのフレームが、電力校正領域(Power Calibration Area)、プログラム・メモリ領域または導入領域(Lead-In Area)に関する時間コードを含むことを意味し、これら総てはプログラム（記録可能な）領域の前に設けられる。他のMSB値は、ATIPフレームが特殊な制御コードを含むことを規定するために使用される。これらのコードは、例えば、ディスク10に関する最適な書き込み電力、参照速度、ディスク・アプリケーション・コード、ディスク形式および副形式、導入領域の開始位置またはディスク10に関する導出領域(Lead-Out Area)の開始位置を指示するために使用される。

【0022】プログラム可能なCD-ROM光学ディスクのROM領域において、溝は、データをアドレスするディスク10およびデータをプログラムするディスクに対応してくぼんだ形状で(depression)更に変調される。CD上でオーディオでない情報が格納されているフォーマットは、「イエロー・ブック」(Yellow Book)規格として知られている。イエロー・ブックでは、CD上のデジタル・データは、インデックスされたトラックに組織化され、誤り訂正符号(C1およびC2誤り訂正と呼ばれる)および組織化されたブロックにおけるサブコード・データとインターリーブされる。ディスク10を通じて、インターリーブされたサブコード情報は、現在のトラックおよびディスク10全体の両者に関して、分、秒、フレームにおける現在位置を定める。

【0023】標準的なCD-ROMモード1データ・セクタは、12バイトの主コード同期フィールド、3バイト・アドレス、1バイト・モード、2048バイトのユーザ・データ、4バイト誤り検出符号、8バイトのゼロ

(5)

特開2002-304808

7

8

(ZEROS)および276バイトの誤り訂正符号より成る。このようなCD-ROMセクタ、すなわちCDブロックまたはブロックは、2352バイトより成り、1秒の1/75(七十五分の一)である。この2352バイトは98フレームで搬送され、各フレームは24バイトのデータ・セクタを含む。さらに、各フレームは、4バイトのC2誤り訂正、4バイトのC1誤り訂正および1バイトのサブコード・データより成る。1バイトのサブコード・データは、サブコードP、Q、R、S、T、U、VおよびWフィールドと呼ばれる8つのサブコード・チャネルに分けられる。各サブコード・チャネルは98ビットより成り、2つの同期ビットと96のデータ・ビットとを含む。

【0024】サブコード・チャネルは従って同様のものであるが、異なる機能および内容を有する。各サブコード・チャネルの最初の2ビットは、サブコード同期パターンS0およびS1を表現する。これらのパターンは、一定の速度でCDを回すCDリーダを同期させるために必要である。

【0025】ディスク10の第1セッション14(ROM領域)は、予め形成された識別番号またはID22を含み、これはマスタ・プロセスの間にATIPチャネルに記録され、そして各プログラム可能なCD-ROMディスクに押印されたデジタル署名である。予め形成されたIDは、サブコード・チャネルおよび主データ・チャネルにも記録される。ATIPチャネルでは、その値は、1つ又はそれ以上の特定の制御コードを利用して、導入領域に記録される。例えば、ディスク・アプリケーション・コード、ディスク形式、ディスク10に関する最適な書き込み電力、参照速度、導入領域の開始位置(オレンジ・ブックにより規定されるような特殊情報2に記録される)、ディスク10に関する導入領域の開始位置(オレンジ・ブックにより規定されるような特殊情報3に記録される)、またはオレンジ・ブックにより定められる他の特殊または付加的な情報は、ディスク製造者に既知の特殊な値に設定されることが可能である。これらの値は単独で又は組み合わせて、予め形成されたID22コードを算出するために使用可能である。さらに、予め形成されたID22コードは、導入部の1つ又はそれ以上のサブコード・データ・チャネルに格納され得る。これらのコードは、既知の絶対アドレスを利用して特定のセクタにおける主データ・チャネル内で反復される。

【0026】ディスク10は第2セッション16を含み、CD-WOまたはCD-RWライタのような再記録可能な光学ディスク技術を利用して書き込まれたものである。ディスク10は、第3セッションを含むことも可能であり、あるいは更に後続の書き込み済みセッション(written session)を含むことも可能である。ディスク10は、ユーザの再記録可能な領域20をも包含する。

記録済みのセッションに含まれているものは、固有の識別番号またはID24および暗号化された実行可能な(executable)パッケージ30であり、ID24は1つ又はそれ以上の既知の絶対セクタ・アドレスにおける第2セッションに書き込まれる。

【0027】図2を参照するに、本発明で使用する実行可能なプログラムを暗号化する手法の1つが示されている。実行可能なパッケージはディスク10に書き込まれる。暗号化されたパッケージは6つの実行可能なプログラム30を含み、これはディスク10において当初の実行可能なプログラム40と同一名称を有する。パッケージ30は、最初に走るラッピング(wrapping)ソフトウェアを含む。このパッケージは、プログラムが走っている際に、ハッキング・ソフトウェアの存在を検査するサブルーチン34も含む。また、データ、命令または両者より成る多形態セクション36も存在する。假して多形態コードは、同一結果に導く複数の経路を提供するが、プログラムが実行される各々の場合に異なる経路をたどるように構成される。多形態コードは、そのプログラムに対するリバース・エンジニアリングを一層困難にするために使用される。暗号解除ルーチン38は、プログラム可能なCD-ROMに格納されたデータ(特に、予め形成されたID22および固有のID24)を利用するために指定され、実行可能なもの40およびセキュリティ・テーブル42の暗号化を解除する。

【0028】図3を参照するに、ユーザの実行可能なプログラムを暗号化するために必要なステップが示され、それを暗号化するためにプログラム可能なCD-ROMの特性を利用する。これは、本願で詳細に説明される様々な本願実施例で使用可能である。ステップ48において、プログラム可能なCD-ROM上に又は局所的なハード・ドライブ上もしくは配信ネットワーク上にマスタされた(mastered)暗号化プログラム可能なCD-ROMが、コンピュータのメモリ内に読み込まれる。ステップ50において、暗号化を要する実行可能なファイルがメモリに読み込まれる。ステップ52において、ソフトウェア・アプリケーションを並布する者またはプログラム可能なCD-ROMを利用する存在として定められる顧客は、マスタされたプログラム可能なCD-ROMディスクをCD-ROMライターに置く。

【0029】顧客が暗号化されるべきファイルを指定することによって開始する。これらのファイルは、データおよび実行可能なプログラムの両者または実行可能なプログラムだけを含み得る。その後顧客は、各ファイルについて所望のセキュリティ・レベルを指定し(ステップ54)、セキュリティ情報を含むテーブルを作成する(ステップ56)。

【0030】その後顧客は、暗号化されたソフトウェアが書き込まれるべきプログラム可能なCD-ROMディスクに関する予め形成されたID22および固有のID

(5)

特開2002-304808

9

19

24に対応する情報を入力する。他の実施例にあっては、これらの値は、それらが記録される任意の場所からプログラム可能なCD-ROMから読み出される。セキュリティ・ソフトウェアが予め形成されたID22および固有のID24を取得すると、ステップ62において、それらを共に利用して暗号キーを作成する。暗号化プログラム63は、ステップ64においてその暗号キーを利用し、実行可能なファイルおよびセキュリティ・レベル・テーブルを暗号化する。ステップ64で暗号化されたファイルは、その後ステップ70においてラッパー(w 10 rapper)プログラムにデータ・ファイルとして付加される。ラッパー・プログラムは、セキュリティ・テーブルにおける指定によって許可されるようなディスク10からの予め形成されたID22および固有のID24を読み込むのに必要なサブルーチンと、プログラムが走っているコンピュータのメモリ内にリバース・エンジニアリング・ツールが存在することを検出し、それらが検出された場合には実行を中断させるサブルーチンと、ソフトウェア・アプリケーションの暗号化解除および実行を開始するサブルーチンを含む。ステップ72において、ラ 20 ップされた実行可能パッケージは、書き込み可能セッション(16または18)においてプログラム可能なCD-ROMディスクに書き込まれる。

【0031】暗号作成法および暗号化機能は当該技術分野で周知である。これに関し、Applied Cryptography, B.Schneier, John Wiley and Sons, Inc., New York, 1996に適切な記載があり、この内容は本願でも使用可能である。本実施例では、以下の表記方法を採用する：

表1

暗号化表記

記号	意味
P	暗号化されるべきプログラム
E	暗号化関数
B	予め形成されたID
U	固有のID
I	連結したID=BU
X	暗号化されたプログラム= $E(P, I)$

本発明に関し、以下の条件を満足する任意の暗号化関数が利用可能であり、それは： $E(P, I)$ の計算が実行可能に適切であること、すなわちEが多項式タイム(poly 40 nomial time)で計算可能であること； $E^{-1}(X, I)$ の計算に関する多項式タイム・アルゴリズムが既知であって実行可能に適切であること；暗号化関数E(およびその逆関数に相当する E^{-1})が、その計算の際に提供される可変なキーIを利用すること；および暗号化/暗号解除プロセスを通じて良好でないプログラム $P' \neq E^{-1}\{E(P, I), I\}$ を形成してしまう蓋然性が非常に小さいこと、である。

【0032】暗号化のステップは以下のとおりである：

1. 予め形成されたID Bおよび固有のID Uを取 50

得する；

2. 2つのIDが連結され($I=BU$)、暗号化/暗号化解除キーIを求める；

3. 暗号化アルゴリズムEで連結されたIDが使用され、暗号化されたプログラム $X=E(P, I)$ を計算する；

暗号化解除のステップは以下のとおりである：

1. 予め形成されたID Bおよび固有のID Bを取得する；

2. 2つのIDが連結され($I=BU$)、暗号化/暗号化解除キーIを求める；

3. 暗号化解除アルゴリズム E^{-1} で連結されたIDが使用され、当初のプログラム $P=E^{-1}(X, I)$ を計算する；

図4を参照するに、本発明の第1実施例に関するブロック図が示される。マスタ・コンパクト・ディスクに関する周知のマスタ技術を利用して、プログラム可能なCD-ROMディスクがマスタされる(ステップ80)。プログラム可能なCD-ROMは第1セッション14を含むが、それに加えて他のマスタ・セッションを含むことも可能である。マスタ・ディスクに含まれるものは、予め形成されたID22である。その後ステップ82において、マスタ・ディスクを利用して、標準的なスタンプ(stamp)手法によりプログラム可能なCD-ROMディスクを製造する。この時点では、多数の同一のプログラム可能なCD-ROMディスクが存在する。

【0033】その後ディスク10は各自の識別子を利用して書き込まれる。ステップ84において、固有のID 24が形成される。固有のID24は、ディスク10の製造順によって定められるところの連続的に定められた番号とすることが可能であり、完全にランダムな番号とすることも可能であり、または予め形成された番号のテーブルから選択することも可能である。他の好適な実施例では、その番号はアルゴリズムによって更に処理され、そのアルゴリズムは、有効な番号(valid number)はとり得る番号の範囲内の小さな部分にのみ対応しているように使用番号(actual number)を生成可能である。この場合、有効な番号は、そのような生成アルゴリズムを知ることによってのみ作成可能である。また、この場合は、検査アルゴリズムを提供し、例えば周知の公開キー、プライベート・キー暗号化および署名の手法を利用することによって、番号を認めることも可能である。他の実施例では、その番号はハードウェア身元確認により生成され、特定のコンピュータに関連付けられる。(この点については、例えばG'Connor et al., U.S. 5,745,568があり、本願でも使用可能である。)他の実施例では、固有のID24が特定のアプリケーションに関連付けられ、このため同一の固有の識別番号が複数のディスク10上で使用される。固有のID24は、書き込み済みセッションとなるISO9660両立可能ファイル

11

・イメージを作成するために使用される（ステップ86）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のID24を利用して修正され（ステップ88）、ステップ90において第2セッション16としてディスク10に加圧されずに書き込まれる。なお、このセッションは第3またはそれ以降のセッションとして書き込まれることも可能である。この時点において、各ディスク10は、各自自身の識別子を含み、特有のものとなる。

【0034】顧客は暗号化に備えてディスク10を用意する。この段階は、ステップ74として図示され、図3で詳細に説明したセキュリティ・ソフトウェアによって実行される複数のステップより成る。固有のID24は、第2セッション16における既知の絶対セクタ・アドレスから読み取られる（ステップ92）。暗号化は、ステップ76として図示され、図3で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク10上の第3セッション18にラップされた実行可能なものが書き込まれる（ステップ94）。

【0035】図5を参照するに、本発明の第2実施例のブロック図が示され、固有のID24および暗号化された実行可能なもの40が同じセッションに書き込まれている。これは、図4で説明したものと同一ステップをいくつか含んでいるが、その順序が異なる。プログラム可能なCD-ROMディスクは、マスタ・コンパクト・ディスクに関して周知のマスタ技術を利用してマスタされる（ステップ80）。プログラム可能なCD-ROMは第1セッション14を含むが、さらに他のマスタ・セッションを含むことも可能である。ディスク10に含まれているものは予め形成されたID22である。その後ステップ82において、マスタ・ディスクを利用して、標準的なスタンプ手法によりプログラム可能なCD-ROMディスクを製造する。この時点では、多数の同一のプログラム可能なCD-ROMディスクが存在する。

【0036】顧客は暗号化に備えてディスク10を用意する。この段階は、ステップ74として図示され、図3で詳細に説明したセキュリティ・ソフトウェアによって実行される複数のステップより成る。固有のID24がステップ84で形成される。固有のID24は完全にランダムな番号とすることが可能であり、予め形成された番号のテーブルから選択することも可能である。固有のID24は、書き込み済みセッションとなるISO9660両立可能ファイル・イメージを作成するために使用される（ステップ86）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のID24を利用して修正される（ステップ88）。ステップ74で読み込んだ予め形成されたID22と共に、固有のID24を利用して、暗号化を行う。暗号化は、ステップ76として図示され、図3で詳細に説明した多数のステップより成る。暗号化が完了すると、ディ

(7)

特開2002-304808

12

スク10上の第3セッション18にラップされた実行可能なものが書き込まれる。

【0037】図6を参照するに、本発明によるエンド・ユーザで実行するための方法が示される。まず、エンド・ユーザはディスク10をCD-ROM、CD-RまたはCD-RWドライブにディスク10を挿入する（ステップ100）。ディスク10上で実行可能なプログラムが自動的に走り出したりは選択される（ステップ102）。プログラムはまず対ハッキング(anti-hacking)サブルーチン34を使用して、ハッキングまたはコピー・プロテクト対策を打ち破るために使用され得るカーネル・デバッグ・ソフトウェア(kernel-debugging software)の検査を行う（ステップ104）。そのようなプログラムが存在すると、そのプログラムはユーザにエラー・メッセージを示し、自動的に停止する（ステップ106）。

【0038】そのようなハッキング・ソフトウェアがエンド・ユーザのシステムに存在しない場合は、ステップ108において暗号化解除プログラムがドライブIDを読み出す。ステップ110において、暗号化解除プログラムは、そのドライブに対して、ATIP信号から予め形成されたID22を読み出すための命令を発行する。暗号化解除プログラムは、そのドライブに対して、サブ・コードから予め形成されたID22を読み出すための命令を発行する（ステップ112）。ステップ114において、暗号化解除プログラムは、主データ・チャネルの既知の絶対セクタ・アドレスから予め形成されたID22を読み出すための命令を発行する。そして、ステップ116において、暗号化解除プログラムは、そのドライブに対して、第2の（後続の）セッションの主データ・チャネルの既知の絶対セクタ・アドレスから固有のID24を読み出すための命令を発行する。

【0039】ステップ118において、暗号化解除プログラムは、ステップ116で読み込んだ固有のID24と、ステップ110でATIPから読み込んだ予め形成されたID22とを連結する。ステップ120において、その連結された結果を暗号化解除キーとして利用して、ラップされたソフトウェア32の暗号化を解除する。ステップ122において、プログラムは、その暗号化解除が有効であるか否かを判定する。これを行ういくつかの手法が存在し、例えば、暗号化解除されたプログラム内のフラグを探索したり、オペレーティング・システム固有のコードが暗号化解除された実行可能なものの中に存在するか否かを検査することが可能である。暗号化解除が成功すると、当初の実行可能なものが開始される（ステップ124）。

【0040】暗号化解除に失敗すると、暗号化解除プログラムは、ステップ108で読み出したドライブIDを利用して、そのドライブがATIPを読み出し得るべきか否かを判定する（ステップ126）。ドライブがAT

(8)

特開2002-304808

13

IP包含リストにあれば(そのドライブがATIPを読み出し得るべきであれば)、プログラムはユーザにエラー・メッセージを示し、停止する(ステップ106)。ドライブがATIP包含リストになければ、暗号化解除プログラムは、ステップ56で記録したセキュリティ・テーブルを参照する(ステップ128)。プログラムのセキュリティ・レベルが最高レベルに設定されていた場合は、サブコードにおける予め形成されたID22を使用することは認められず、プログラムはユーザにエラー・メッセージを示し、停止する(ステップ106)。サブコードからの予め形成されたID22が許容される場合は、暗号化解除プログラムは、ステップ116で読み出した固有のID24と、ステップ112でサブコードから読み出した予め形成されたID22とを連結させる(ステップ130)。そして、ステップ132においてラップされたソフトウェア32の暗号化を解除する暗号化解除キーとして、その連結された結果物を使用する。その後プログラムは暗号化解除が有効であるか否かを判定する(ステップ134)。暗号化解除が成功すると、当初の実行可能なものが開始される(ステップ124)。

【0041】暗号化解除に失敗すると、暗号化解除プログラムは、ステップ108で読み出したドライブIDを利用して、そのドライブがサブコードを読み出し得るべきか否かを判定する(ステップ136)。ドライブがサブコード包含リストにあれば(それがサブコードを読み出し得るべきであれば)、プログラムはユーザにエラー・メッセージを示し、停止する(ステップ106)。ドライブがサブコード包含リストになければ、暗号化解除プログラムは、ステップ56で記録したセキュリティ・テーブルを参照する(ステップ138)。プログラムのセキュリティ・レベルが高いレベルに設定されていた場合は、主データにおける予め形成されたID22を使用することは認められず、プログラムはユーザにエラー・メッセージを示し、停止する(ステップ106)。主データからの予め形成されたID22が許容される場合は、暗号化解除プログラムは、ステップ116で読み出した固有のID24と、ステップ114で主データから読み出した予め形成されたID22とを連結させる(ステップ140)。そして、ステップ142においてラップされたソフトウェア32の暗号化を解除する暗号化解除キーとして、その連結された結果物を使用する。その*

14

*後プログラムは暗号化解除が有効であるか否かを判定する(ステップ144)。暗号化解除が成功すると、当初の実行可能なものが開始される(ステップ124)。暗号化解除に失敗すると、エラー・メッセージがユーザに示され、プログラムおよび全プロセスが終了する(ステップ106)。

【0042】暗号化解除が成功する任意の時点において(ステップ122、134、144)、当初の実行可能なものが開始される(ステップ124)。暗号化解除プログラムは背景に残り(ステップ148)、プログラムは実行され(ステップ146)および抜け出す(ステップ150)。当初のプログラムが抜け出ると、暗号化解除プログラムは、メモリおよび当初プログラムの使用したハード・ドライブの領域をクリアし(ステップ152)、終了する(ステップ154)。

【図面の簡単な説明】

【図1】図1は、本発明によるコピー・プロテクトを有するコンパクト・ディスクの平面図である。

【図2】図2は、コピー不可能にアプリケーションを暗号化するソフトウェア手法の概略図である。

【図3】図3は、暗号化されたソフトウェアを形成するためのステップを示すブロック図である。

【図4】図4は、コピー・プロテクトがCDにどのように提供されるかの一例を示すブロック図である。

【図5】図5は、コピー・プロテクトがCDにどのように提供されるか他の例を示すブロック図である。

【図6】図6は、CDが読み込まれる場合に、コピー・プロテクトがどのように機能するかを示すブロック図である。

【図7】図7は、ここに開示したコピー・プロテクトが、それを破ろうとする方法をどのようにして阻止するかを示すブロック図である。

【符号の説明】

- 10 光学ディスク
- 14 第1セッション
- 16 第2セッション
- 18 第3セッション
- 20 再記録可能な領域
- 22 予め形成されたID
- 24 固有のID
- 30 パッケージ

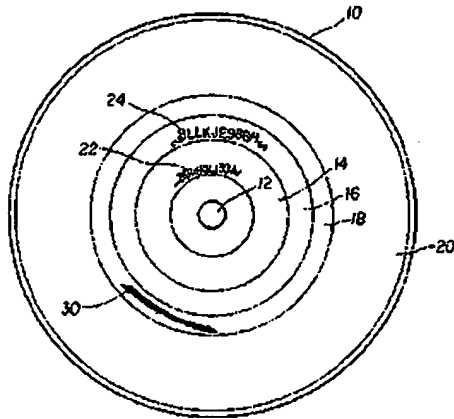
【図6】



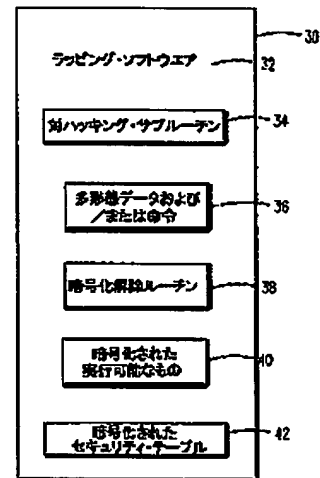
(9)

特開2002-304808

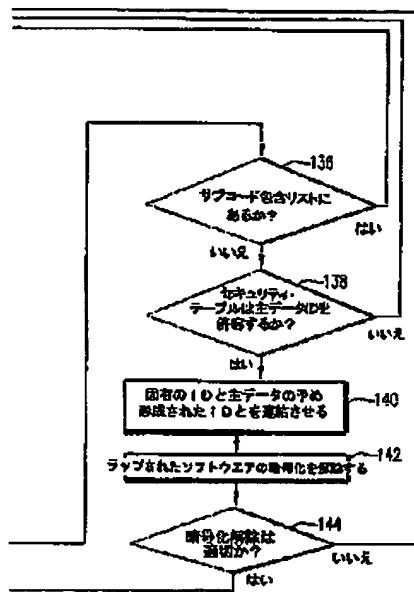
【図1】



【図2】



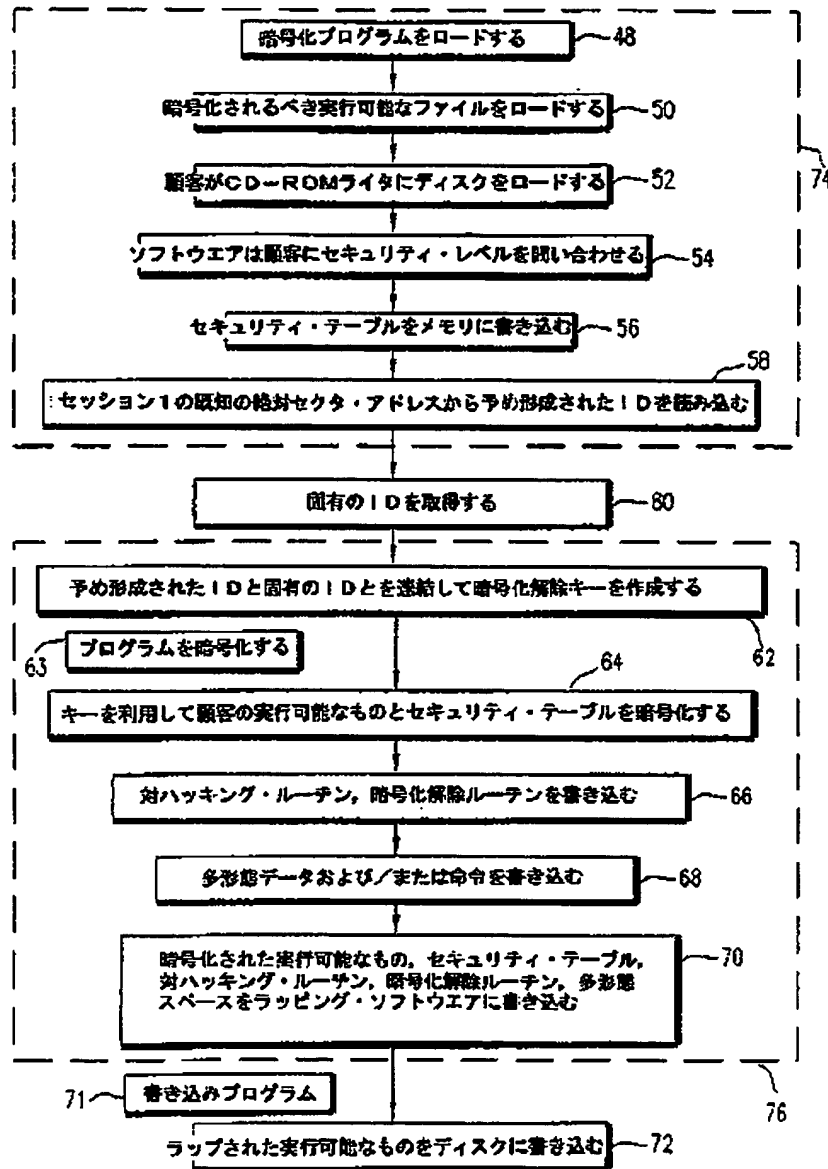
【図6B】



(10)

特開2002-304808

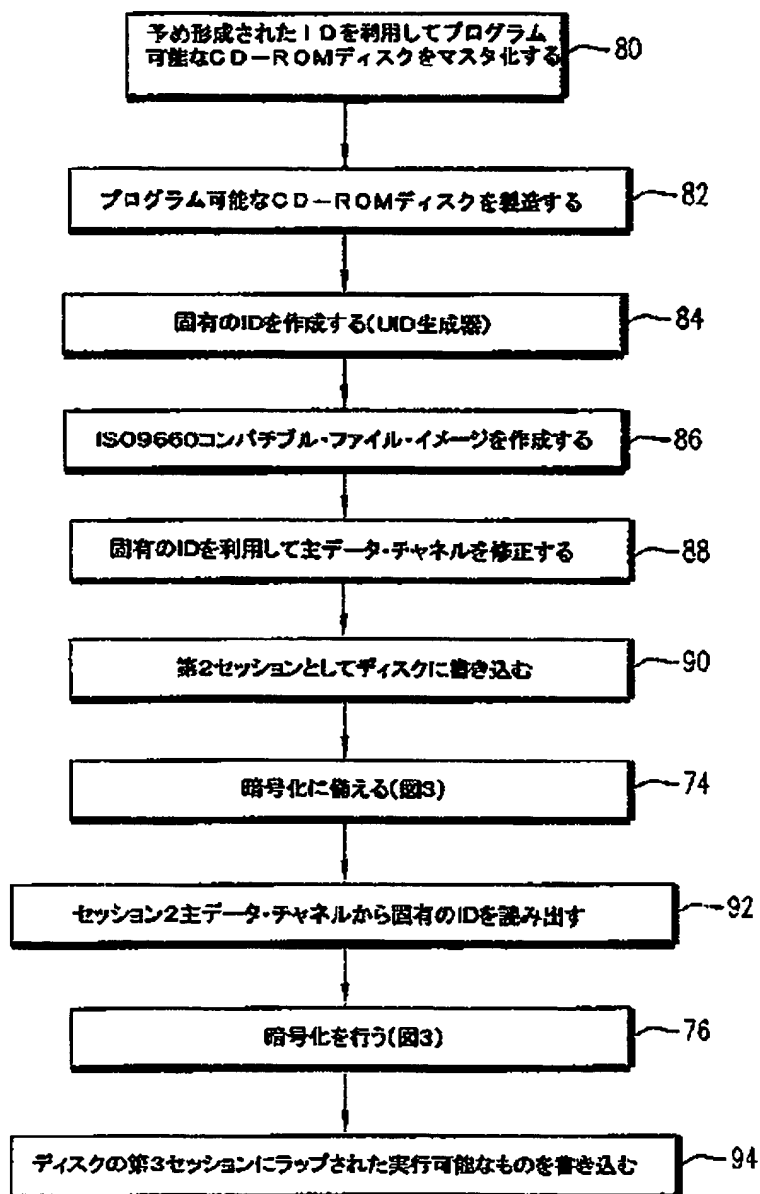
【図3】



(11)

特開2002-304808

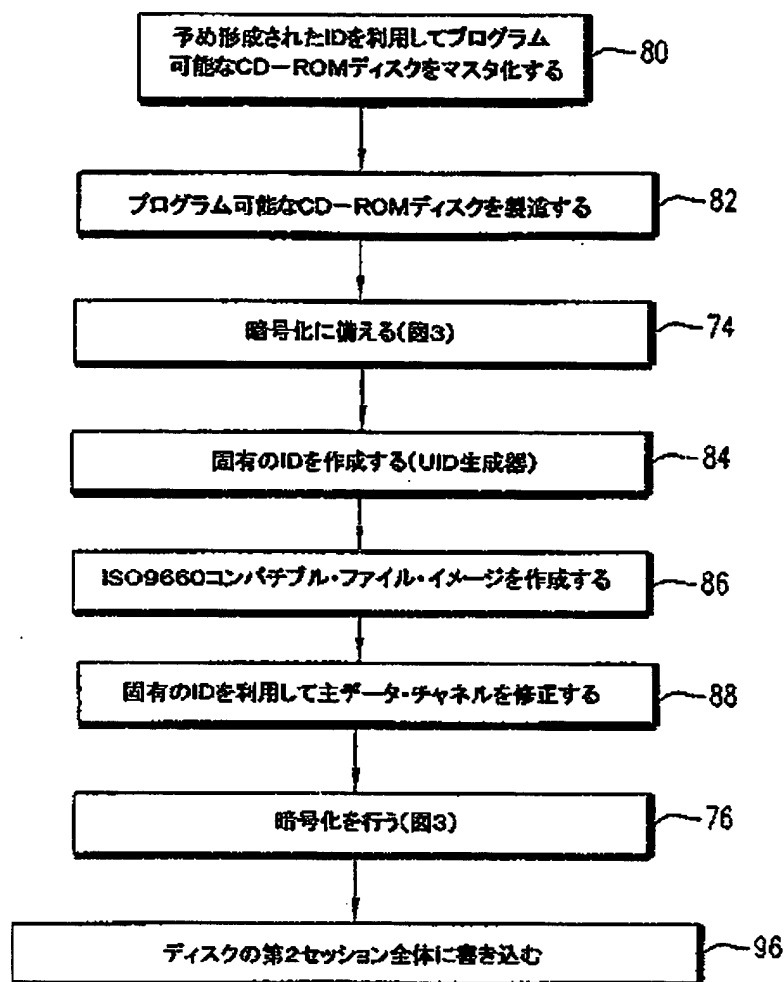
〔図4〕



(12)

特開2002-304808

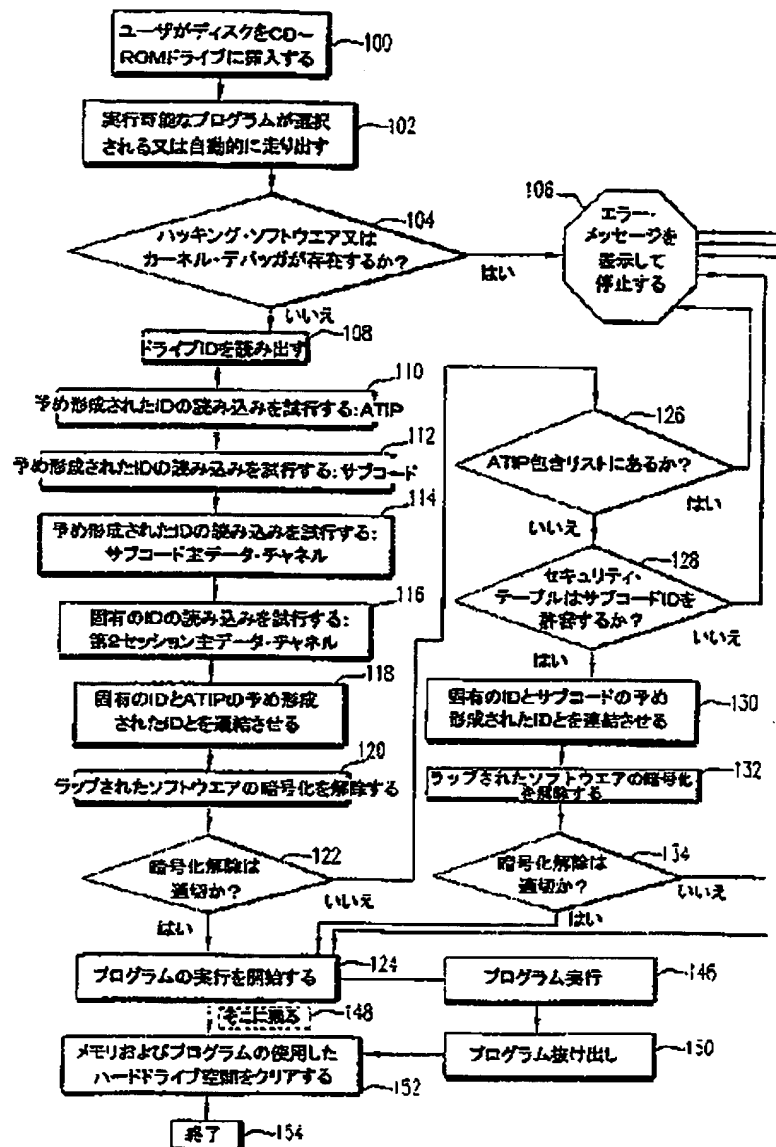
【図5】



(13)

特開2002-304808

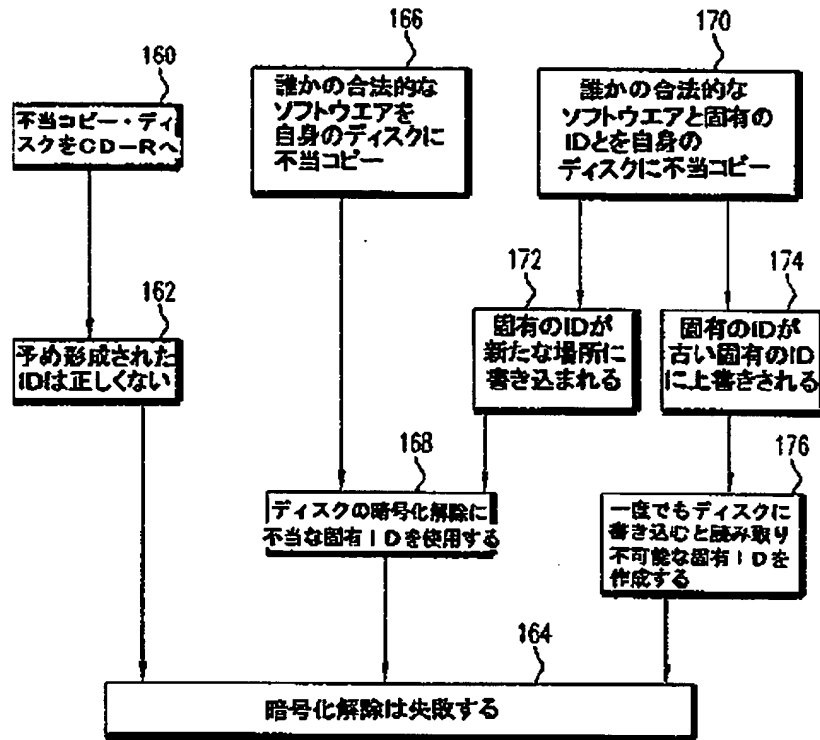
【図6A】



(14)

特開2002-304808

【図7】



フロントページの続き

(51)Int.Cl.	識別記号	F I	キーワード (参考)
G 1 1 B 7/007		G 1 1 B 20/12	
20/12		G 0 6 F 9/06	6 6 0 G
(72)発明者	ブルース エル ハ	F ターム (参考)	5B017 AA06 AA07 BA07 CA09 CA15
	アメリカ合衆国 ニューヨーク 14580		5B076 FA05 FC06
	ウェブスター レイク・ロード 1072		5D044 BC04 CC04 DE49 DE50 DE54
			DE55 GK17
			5D090 AA01 BB04 CC12 CC14 FF09
			GG03 GG32 HH01

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.